Aufgabe 1. Konstruiere Wahrheitstafeln für die folgenden Formeln:

$$\text{(a)}((A \wedge B) \wedge (\neg B \vee C)) \qquad \text{(b)}((A \leftrightarrow B) \leftrightarrow C)$$

Aufgabe 2. Zeige anhand von Wahrheitstafeln, daß die Aussageformen

$$(A \vee B) \to C \quad \text{und} \quad (A \to C) \wedge (B \to C)$$

äquivalent sind (= für jede Belegung der Variablen den gleichen Wahrheitswert ergeben).

Aufgabe 3. Graf Orlofsky wurde letzten Donnerstag zwischen 11:00 und 13:00 aus dem Fenster seiner Jacht ins Meer gestürzt und ist ertrunken. Der Koch ist um 12:00 vom Vordeck ins Innere der Jacht gekommen und hat nichts bemerkt. Um am Koch vorbeizukommen, muß der Mörder entweder am Vormittag mit einem Schlüssel über den Steg und durch die Eingangstür in die Jacht gekommen sein oder am Nachmittag aus einem Boot direkt durchs Fenster eingestiegen sein. Inspektor Kottan vermutet einen der drei Erben Alois, Bob oder Clemens als Mörder. Alois hat als einziger einen Schlüssel, kann aber wegen seines Gipsfußes nicht durchs Fenster gestiegen sein. Alois und Bob haben beide ein Alibi für den Vormittag, aber keines nach 12 und Clemens hat kein Alibi für die Zeit vor 12, wohl aber am Nachmittag. Wer von den dreien kommt als Mörder in Frage?

Hinweis: Sei M. der Mörder. Bilden Sie zunächst Aussagen wie S: "M hat einen Schlüssel", F: "M kann durchs Fenster steigen.", V: "M hat am Vormittag ein Alibi.", N: "M hat am Nachmittag ein Alibi." Finden Sie weiters Folgerungen, die sich aus dem Text ergeben, wie $\bar{V} \vee \bar{N}$, $F \vee S$, $V \to F$, $N \to S$, und überprüfen Sie nacheinander die Hypothesen, daß A, B, oder C der Mörder ist.

Aufgabe 4. Die Wahl in Kakanien hat eine Koalition aus der Vermögendenpartei (VPK) und die Partei der Pudelfreunde (FPK) ergeben. Die Ministerien für Finanzen, Digitalisierung und Pferdeangelegenheiten werden nach folgenden Regeln besetzt:

1. Die VPK bekommt mindestens ein Ministerium.
2. Die VPK bekommt nicht zugleich das Digitalisierungs- und das Pferdeministerium.
3. Wenn die FPK das Digitalisierungsministerium bekommt, dann auch das Pferdeministerium.
4. Wenn die VPK das Finanz- oder das Digitalisierungsministerium bekommt, aber nicht beide, dann bekommt sie auch das Pferdeministerium.

Wie werden die Ministerien besetzt?

Aufgabe 5. Ist der folgende Schluß korrekt?
(„Wer von der Quantenmechanik nicht schockiert ist, der hat sie nicht verstanden" (Nils Bohr) ∧ „Niemand versteht die Quantenmechanik" (Richard Feynman)) → „Niemand ist von der Quantenmechanik schockiert"

Aufgabe 6. Formalisiere folgende Aussagen mittels Aussagenlogik.

- Von A, B und C gilt genau eines.
- Von A, B und C gelten genau zwei.
- Von A, B und C gilt mindestens eines.

Aufgabe 7. Die folgenden Aufgaben sind Schritt für Schritt unter Anwendung der logischen Schlußregeln (s. Internetseite) und ohne Verwendung von Wahrheitstabellen zu lösen.

(a) Zeige, daß die folgenden Aussageformen äquivalent sind:

$$A \to (B \to C) \Longleftrightarrow B \to (A \to C)$$

(b) Zeige, daß der folgende Ausdruck eine *Tautologie* ist, d.h., immer erfüllt ist:

$$(A \to B) \wedge (B \to C) \to (A \to C)$$

Aufgabe 8. Seien x und y reelle Zahlen.

(a) Formuliere die folgenden Aussagen in Umgangssprache.
  (i) $\forall x \exists y : x = y^3$
  (ii) $\exists x \forall y : xy \neq 0$
  (iii) $\forall x \exists y : x \geq y$
  (iv) $\exists x \forall y : x \geq y$

(b) Welche der Aussagen sind wahr?

(c) Verneine die Aussagen und forme sie solange um, bis sämtliche Quantoren links stehen.

Aufgabe 9. Zu zwei Mengen M und N betrachten wir die Aussagen

A: Jedes Element von M liegt auch in N.
B: Kein Element liegt in beiden Mengen zugleich.
C: Nicht alle Elemente von N liegen auch in M.

(a) Formuliere diese Aussagen mit Quantoren und Junktoren und forme sie solange um, bis sämtliche Quantoren ganz links stehen.

(b) Gib für jede einzelne Aussage passende Mengen M und N an, die sie erfüllen.

(c) Gibt es Mengen M und N, die alle drei Aussagen erfüllen?

Aufgabe 10. Welche der folgenden Aussagen sind allgemeingültig?
Wahre Aussagen beweisen mit Venndiagramm oder logischen Argumenten, falsche Aussagen durch Gegenbeispiel nachweisen.

(a) $\varnothing \subseteq \varnothing$
(b) $\varnothing \in \varnothing$
(c) $\varnothing \subseteq \{\varnothing\}$
(d) $\varnothing \in \{\varnothing\}$
(e) $(A \in B) \wedge (B \subseteq C) \to (A \in C)$
(f) $(A \notin B) \wedge (B \subseteq C) \to (A \notin C)$
(g) $(A \in B) \wedge (B \in C) \to (A \in C)$

Aufgabe 11. Welche der folgenden Aussagen sind allgemeingültig?
(Gegenbeispiel oder Beweis mit (i) Venndiagramm und (ii) logischen Argumenten)

(a) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$
(b) $(A \setminus B) \setminus C = A \setminus (B \cup C)$
(c) $(A \setminus B) \setminus C = A \setminus (B \setminus C)$

Aufgabe 12. Untersuche die folgenden Relationen auf die Eigenschaften Reflexivität, Symmetrie, Antisymmetrie und Transitivität und stelle fest, ob jeweils eine Äquivalenzrelation oder Halbordnungsrelation vorliegt.

(a) $X = \mathbb{N}$, $mRn \Longleftrightarrow m - n = 7$
(b) $X = \mathbb{N}$, $mRn \Longleftrightarrow \mathrm{ggT}(m, n) = 16$
(c) Menge $X = \mathbb{Z}$, Relation $xRy \Longleftrightarrow x = |y|$.
(d) $X = \mathbb{R}$, $xRy \Longleftrightarrow x \cdot y \geq 0$
(e) $X = \mathbb{N}$, $mRn \Longleftrightarrow 2 | (m + n)$
(f) Menge $X = \{a, b, c, d\}$, Relation R entsprechend der folgenden Tabelle:

	a	b	c	d
a	×	×	×	×
b		×		
c			×	
d		×	×	×

(g) $X = \{a, b, c\}$, $R = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$. Was muss aus der Relation R entfernt werden, damit sie antisymmetrisch wird? (Es gibt mehrere Möglichkeiten!)

Aufgabe 13. Zeige daß durch

$$xRy \iff x - y \in \mathbb{Z}$$

eine Äquivalenzrelation auf $\mathbb{R}$ definiert wird, bestimme die Äquivalenzklassen und eine Repräsentantensystem.

Aufgabe 14. Sei $X = \{0, 1, 2, 3\}$ mit der Relation $\mathrm{R} = \{(0,1), (0,2), (1,1), (1,3), (2,2), (3,0)\}$. Bestimme den transitiven Abschluß $\bar{R}$, d.h., die kleinste transitive Relation, die R als Teilmenge enthält.

Aufgabe 15. Sei $A = \{1, 2, 3, 4, 5\}$. Bilde die kleinste Äquivalenzrelation auf A, die die Elemente $(1, 3)$, $(4, 3)$ und $(2, 5)$ enthält, bestimme die Äquivalenzklassen und ein Repräsentantensystem.

Aufgabe 16. Für welche $n \in \mathbb{N}$ ist $43 \equiv 1 \mod n$?

Aufgabe 17. Stelle fest, für welche $m \geq 2$ durch

$$x \sim_m y \iff m \text{ teilt } x + y$$

eine Äquivalenzrelation auf $X = \mathbb{Z}$ definiert wird.

Aufgabe 18. Bestimme alle Zahlen $m, n \in \mathbb{N}$, für die gilt

(a) $\mathrm{ggT}(m, n) = 7$ und $\mathrm{kgV}(m, n) = 2730$.
(b) $\mathrm{ggT}(m, n) = 1$ und $\mathrm{kgV}(m, n) = 36$.

Hinweis: Die Identität $\mathrm{ggT}(m, n) \cdot \mathrm{kgV}(m, n) = m \cdot n$ darf verwendet werden.

Aufgabe 19. Seien $m, n \in \mathbb{Z}$. Zeige:

(a) Wenn es Zahlen $a, b \in \mathbb{Z}$ gibt sodaß $am + bn = 1$, dann ist $\mathrm{ggT}(m, n) = 1$
(b) Sei $g = \mathrm{ggT}(m, n)$, dann ist $\mathrm{ggT}(m/g, n/g) = 1$.

Aufgabe 20. Seien $m \in \mathbb{N}$ und $x, y, x', y' \in \mathbb{Z}$. Zeige: Wenn

$$x \equiv x' \mod m \qquad \text{und} \qquad y \equiv y' \mod m,$$

dann gilt auch

$$x + y \equiv x' + y' \mod m \qquad \text{und} \qquad xy \equiv x'y' \mod m.$$

Aufgabe 21. Finde mithilfe des euklidischen Algorithmus für jedes der folgenden Zahlenpaare (m, n) den größten gemeinsamen Teiler d und Zahlen a und b, sodass $am + bn = d$.

(a)	$(233, 89)$	(b)	$(425, 2023)$
(c)	$(377, 144)$	(d)	$(228, 141)$
(e)	$(144, 347)$	(f)	$(231, 142)$

Aufgabe 22. Seien $m, n \in \mathbb{N}$, sodass $\mathrm{ggT}(m, n) = 1$. Zeige, dass $\mathrm{ggT}(m + n, m - n) = 1$ oder 2.

Aufgabe 23. Finde (mit dem Computer[1]) die kleinste Zahl $n \in \mathbb{N}$, für die $n^2 + n + 41$ *keine* Primzahl ist.

Aufgabe 24. Zeige: Wenn n keine Primzahl ist, dann kann auch $2^n - 1$ keine Primzahl sein.

Aufgabe 25. Zeige: Wenn $k \geq 6$ und sowohl $k - 1$ als auch $k + 1$ Primzahlen sind, dann ist k durch 6 teilbar.

Aufgabe 26. Verfasse einen möglichste effizienten Algorithmus, der zu einer gegebenen Zahl n und einer Liste aller Primzahlen $p \leq n$ die Primfaktorzerlegung von n ermittelt.
Führe den Algorithmus für das Beispiel $n = 1911$ per Hand durch.

[1] Der entsprechende Code/die Vorgangsweise ist zu präsentieren!

Aufgabe 27. Zeige die *Elferprobe*: Eine Zahl $n \in \mathbb{Z}$ ist genau dann durch 11 teilbar, wenn die alternierende Quersumme durch 11 teilbar ist, d.h., mit der Ziffernentwicklung

$$n = \sum a_i 10^i$$

ist n durch 11 teilbar genau dann, wenn

$$\sum a_i (-1)^i$$

durch 11 teilbar ist.

Aufgabe 28. Eine österreichische IBAN (*international bank account number*) hat immer zwanzig Stellen und sieht folgendermaßen aus:

$$AT\mathit{pp}\ \mathit{bbbb}\ \mathit{bkkk}\ \mathit{kkkk}\ \mathit{kkkk}$$

wobei *bbbbb* die fünfstellige Bankleitzahl, *kkk kkkk kkkk* die (um Nullen ergänzte) herkömmliche Kontonummer ist und *pp* ein Prüfcode zwischen 02 und 98, der so bestimmt wird, dass

$$\mathit{bbbbbkkkkkkkkkk}1029\mathit{pp} \equiv 1 \mod 97.$$

(1029 entsteht aus AT durch addieren von 9 zur Stelle im Alphabet: also $A \to 1 + 9 = 10$, $B \to 2 + 9 = 11$, …, $Z \to 26 + 9 = 35$).
Bestimme die IBAN der folgenden Kontonummer[2]: BLZ: 12345, KtoNr: 7654321

Aufgabe 29. Die maschinelle Verifikation einer IBAN erfordert Rechnungen mit 30bit INT. Auf eingeschränkter Hardware, die diese Operationen nicht beherrscht, kann die Überprüfung schrittweise wie folgt durchgeführt werden:

1. Zerlege die Zahl $N = b_1b_2b_3b_4b_5k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}1029p_1p_2$ in drei Teile $b_1b_2b_3b_4b_5k_1k_2k_3k_4$, $k_5k_6k_7k_8k_9k_{10}k_{11}$, $1029p_1p_2$ (9+7+6 Ziffern).
2. Nehme die ersten 9 Stellen $N_1 = b_1b_2b_3b_4b_5k_1k_2k_3k_4$.
3. Berechne den Rest $r_1r_2 = N_1 \mod 97$.
4. Füge diese beiden Ziffern zu den nächsten 7 Stellen hinzu und bilde die Zahl $N_2 = r_1r_2k_5k_6k_7k_8k_9k_{10}k_{11}$
5. Berechne den Rest $r_3r_4 = N_2 \mod 97$.
6. Füge diese beiden Ziffern zu den verbleibenden Stellen hinzu und bilde die Zahl $N_3 = r_3r_41029p_1p_2$.
7. Der Rest $N_3 \mod 97$ muß 1 ergeben.

(a) Überprüfe die IBAN aus Aufgabe 28 mit dieser Methode.
(b) Zeige, daß der Algorithmus wirklich das gleiche Ergebnis liefert wie die Division der kompletten IBAN modulo 97.

Aufgabe 30. Zeige, daß eine IBAN ungültig wird, wenn

(a) eine Ziffer falsch eingegeben wird.
(b) zwei benachbarte Ziffern vertauscht werden.

Aufgabe 31. Finde, wenn möglich, die folgenden multiplikativen Inversen:

(a) $[5]_{17}^{-1}$ (b) $[14]_{93}^{-1}$
(c) $[51]_{85}^{-1}$ (d) $[15]_{93}^{-1}$

Aufgabe 32. Löse, wenn möglich, das Gleichungssystem

$$x + 2\,y = 4$$
$$4x + 3\,y = 3$$

(a) in $\mathbb{Z}_5$ (b) in $\mathbb{Z}_7$

[2]Bitte kein Geld überweisen, es ist nicht das Konto des Vortragenden und verbessert nicht die Note.

Aufgabe 33. Finde alle Lösungen $x \in \mathbb{Z}$, der folgenden Gleichungen.

(a) $4x + 3 \equiv 1 \mod 7$
(b) $4x + 3 \equiv 2 \mod 9$
(c) $6x \equiv 3 \mod 9$
(d) $6x \equiv 4 \mod 9$

Aufgabe 34. Löse das folgende Kongruenzgleichungssystem mithilfe des chinesischen Restsatzes.

$$\begin{aligned} x &\equiv 1 \mod 11 \\ x &\equiv 6 \mod 18 \\ x &\equiv 5 \mod 7 \end{aligned}$$

Aufgabe 35. Zeige, dass die folgende Aussage wahr ist:

$$a \equiv b \mod m \text{ und } a \equiv b \mod n \implies a \equiv b \mod k \quad \text{für} \quad k = \mathrm{kgV}(m_1, m_2)\,.$$

Ist insbesondere $\mathrm{ggT}(m_1, m_2) = 1$, dann gilt also $a \equiv b\ (m_1 m_2)$.
Folgere daraus, daß die Menge aller Lösungen eines Kongruenzgleichungssystems $x \equiv c_i \mod m_i$, $i = 1, 2, \ldots, k$ und $\mathrm{ggT}(m_i, m_j) = 1$, gegeben ist durch $\{x_0 + km \mid k \in \mathbb{Z}\}$, wobei $m = m_1 m_2 \cdots m_k$.

Aufgabe 36. Welche der folgenden Gleichungssystems sind lösbar? Wenn ja, dann bestimme diese. Ist der chinesische Restsatz anwendbar?

$$(a)\quad \begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 9 \\ x &\equiv 1 \mod 10 \end{aligned} \qquad (b)\quad \begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 3 \mod 9 \\ x &\equiv 2 \mod 10 \end{aligned}$$

Aufgabe 37. Berechne ohne Taschenrechner

$$2^{32} \mod 1260$$

Hinweis: $1260 = 4 \cdot 5 \cdot 7 \cdot 9$. Rechne zuerst modulo 4, 5, 7, 9 (Regeln fürs Exponentialrechnen ausnützen, es ist fast nichts zu tun!) und wende am Ende den Chinesischen Restsatz an.

Aufgabe 38. Welche der folgenden Strukturen $(X, \circ)$ bilden Halbgruppen, Monoide, Gruppen? In welchen gilt das Kommutativgesetz? Bestimme ggf. das neutrale Element, die invertierbaren Elemente und die jeweiligen Inversen.

a. $(\mathbb{Q}, \circ)$ mit $x \circ y = x + 2y$
b. $(\mathbb{N}, \circ)$ mit $x \circ y = \max(x, y)$.
c. $(\mathbb{N}, \circ)$ mit $x \circ y = \min(x, y)$.
d. $(\mathbb{N}_0, \circ)$ mit $x \circ y = |x - y|$.
e. $(\mathbb{R} \setminus \{-1\}, \circ)$ mit $x \circ y = x + y + xy$.
f. X beliebig, $x \circ y = x$.

Aufgabe 39.

(a) Berechne $\varphi(10!) = \varphi(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10)$.
(b) Berechne $\varphi(5186)$, $\varphi(5187)$, $\varphi(5188)$.
(c) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 1$.
(d) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 2$.
(e) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 3$.

Hinweis: Wenn $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, dann ist jedes $\varphi(p_i^{k_i})$ ein Teiler von $\varphi(n)$.

Aufgabe 40. Berechne (ohne Taschenrechner), mit Hilfe des Satzes von Euler-Fermat die Potenz

$$2^{(2^{32})} \mod 11\,.$$

Aufgabe 41. Berechne mit dem Satz von Euler-Fermat (ohne Taschenrechner) in $\mathbb{Z}_{60}$

$$[14]^{(2^{32})}$$

Hinweis: Der Satz von Euler-Fermat ist nicht sofort anwendbar (warum?). Man kann aber wie folgt vorgehen: Zerlege $60 = 2^2 \cdot 3 \cdot 5$. Bestimme $[14]^{(2^{32})} \mod 4$, $[14]^{(2^{32})} \mod 3$, $[14]^{(2^{32})} \mod 5$, und verwende den chinesischen Restsatz, um daraus $14^{(2^{32})} \mod 60$ zu bestimmen.

Aufgabe 42. Um Frequenzanalyse zu erschweren, empfiehlt es sich, Buchstabengruppen zu verschlüsseln, z.B. paarweise. Dazu numeriert man die Buchstaben A-Z von 0 bis 25 durch und faßt diese Zahlen als Ziffern in einem Zahlensystem zur Basis 26 auf. Das heißt, unser "Alphabet" besteht aus $26 \cdot 26 = 676$ Buchstabenpaaren:

$$\begin{array}{llll} AA \triangleq 0, & AB \triangleq 1, & AC \triangleq 2, & \dots \quad AZ \triangleq 25 \\ BA \triangleq 26, & BB \triangleq 27, & BC \triangleq 28, & \dots \quad BZ \triangleq 51 \\ CA \triangleq 52, & CB \triangleq 53, & CC \triangleq 54, & \dots \quad CZ \triangleq 87 \\ \vdots & & & \\ ZA \triangleq 650, & ZB \triangleq 651, & ZC \triangleq 652 & \dots \quad ZZ \triangleq 675, \end{array}$$

d.h. dem Buchstabenpaar $b_i b_j$ entspricht die Zahl $i \cdot 26 + j$
Mit diesen Zahlen kann dann weitergerechnet werden, indem z.B. ein Caesar-Schlüssel modulo 676 addiert wird.

(a) Stelle das Wort OKAY mit diesem Zahlencode dar, addiere dazu den Caesar-Schlüssel 84 und wandle den erhaltenen Code in ein verschlüsseltes Wort um.
(b) Entschlüssle das Wort EURSHX mit dem inversen Schlüssel.

Aufgabe 43. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31$, $g = 7$, $a = 13$, $b = 11$.
(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$\begin{array}{ll} g = 8 & p = 29 \\ m = 10 & n = 16 \end{array}$$

Bestimme die geheimen Parameter a, b und den Schlüssel r!

Aufgabe 44. Welche der folgenden Zahlen g, m, n, p sind für eine Schlüsselvereinbarung nach Diffie-Hellman-Merkle geeignet? Berechne gegebenenfalls die geheimen Parameter a und b sowie den Schlüssel s. (Für die Zwischenrechnungen ist ein Computer erlaubt.)

(a) $g = 17$, $m = 29$, $n = 59$, $p = 201$
(b) $g = 10$, $m = 29$, $n = 45$, $p = 199$
(c) $g = 10$, $m = 24$, $n = 6$, $p = 101$

Aufgabe 45. Gegeben sei $m = 1363$.

(a) Welche der folgenden Zahlen sind als öffentliche RSA-Schlüssel geeignet (Begründung!)?

$$r = 21 \qquad r = 23 \qquad r = 25$$

Berechne die zugehörigen inversen Schlüssel.
(b) Wähle einen geeigneten Schlüssel und verschlüssle die Botschaft

"FAKENEWS"

mit der Konvention aus Aufgabe42.
(c) Die folgende Nachricht wurde mit dem Schlüssel $r = 17$, $m = 1363$ verschlüsselt.

$$[579, 304, 816]$$

Finde den inversen Schlüssel s und entschlüssle die Botschaft.

Hinweis: Für die Zwischenrechnungen ist ein Computer erlaubt.

Aufgabe 46. Die Ver- und Entschlüsselungen beim RSA-Verfahren können effizienter gestaltet werden, wenn man die Potenzfunktionen $e_m(x,k) = x^k \mod m$ zunächst die Funktionen $e_p(x,k) = x^k \mod p$ und $e_q(x,k) = x^k \mod q$ berechnet und dann das Ergebnis mit Hilfe des chinesischen Restsatzes ermittelt. Verwende dieses Prinzip, um die folgende Aufgabe ohne elektronische Hilfsmittel zu lösen:
Für den RSA-Algorithmus wurde der öffentliche Schlüssel $m = 119$ und $r = 13$ bekanntgegeben.

(a) Verschlüssle die Nachricht $(14, 42)$.
(b) Berechne den Geheimschlüssel s und entschlüssle die Botschaft.
(c) Berechne eine digitale Signatur für die Nachricht $(33, 5)$.

Aufgabe 47. In diesem Beispiel soll gezeigt werden, dass die Verwendung kleiner Exponenten in öffentlichen Schlüsseln (z.B. aus Effizienzgründen) problematisch sein kann.
Sei $r = 3$ und es sei bekannt, dass die gleiche Nachricht x mit den öffentlichen Schlüsseln $(m_1, r) = (143, 3)$, $(m_2, r) = (391, 3)$ und $(m_3, r_3) = (899, 3)$ zu folgenden Werten verschlüsselt wurde:

$$x^3 \equiv 129 \mod 143$$
$$x^3 \equiv 281 \mod 391$$
$$x^3 \equiv 380 \mod 899$$

Bestimme x, ohne die Schlüssel m_i zu faktorisieren. Wie groß darf x sein, damit diese Methode funktioniert?

Aufgabe 48. Begründe, warum im RSA-Verfahren anstelle von $\phi(m) = (p-1)(q-1)$ auch die Zahl $\lambda(m) = \mathrm{kgV}(p-1, q-1)$ verwendet werden kann.
Hinweis: Chinesischer Restsatz!

Aufgaben der Klausur von 2020, es ist nichts mehr anzukreuzen!

Aufgabe 49. Zeige, dass für beliebige Mengen A und B gilt

$$A \cup (B \setminus A) = A \cup B$$

(a) durch logisches Schließen.
(b) durch Venndiagramme.

Aufgabe 50. Auf $X = \mathbb{R}$ sei die Relation

$$xRy \Longleftrightarrow x - y \in \mathbb{Z}$$

gegeben. Stelle fest (mit **ausführlicher** Begründung), ob die Eigenschaften

Reflexivität
Symmetrie
Antisymmetrie
Transitivität

erfüllt sind und ob es sich um eine Äquivalenzrelation oder Ordnungsrelation handelt, und bestimme ggf. die Äquivalenzklassen.

Aufgabe 51. Bestimme, wenn möglich, die multiplikativen Inversen von 18, 19 und 20 in $\mathbb{Z}_{133}$.

Aufgabe 52. Beschreibe einen Diffie-Hellman-Schlüsselaustausch mit den öffentlichen Parametern $g = 3$ und $p = 11$ und den geheimen Exponenten $a = 7$ und $b = 9$.